

METHOD AND PROGRAM FOR AUTOMATICALLY PROCESSING ANNOYING MAIL IN MAIL SERVER OF MOBILE PHONE

Patent number: JP2003249964

Publication date: 2003-09-05

Inventor: SHIRATO HIROYUKI

Applicant: NEC COMMUNICATION SYST

Classification:

- international: G06F13/00; H04L12/58; G06F13/00; H04L12/58; (IPC1-7): H04L12/58; G06F13/00

- european:

Application number: JP20020046836 20020222

Priority number(s): JP20020046836 20020222

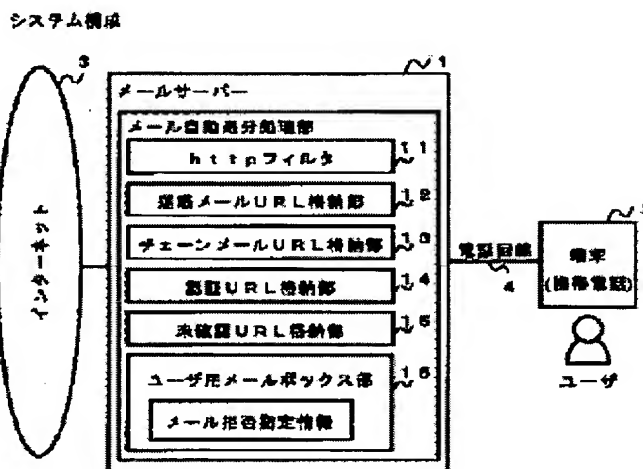
Report a data error here

Abstract of JP2003249964

PROBLEM TO BE SOLVED: To automatically discriminating annoying mails or the like in a mail server of a mobile phone by a prescribed discrimination condition to prevent unnecessary reception by automatic deletion and to allow a user to utilize a system by easy user's setting.

SOLUTION: The mail server of the mobile phone has a step wherein it is checked whether a URL is included in the mail text of a mail received through a network or not and the URL is extracted when included, a step wherein the extracted URL is used to discriminate whether the received mail is an annoying mail or a chain mail, and a step wherein the received mail discriminated as an annoying mail or a chain mail as a result of discrimination is not stored in a mail box for the user and is deleted. The discrimination condition is automatically updated at any time.

COPYRIGHT: (C)2003,JPO



Data supplied from the esp@cenet database - Worldwide

THIS PAGE BLANK (USPTO)

① - ⑦/9

P3014

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-249964

(P2003-249964A)

(43) 公開日 平成15年9月5日 (2003.9.5)

(51) Int.Cl. ⁷	識別記号	F I	テームコード* (参考)
H 0 4 L 12/58	1 0 0	H 0 4 L 12/58	1 0 0 F 5 K 0 3 0
G 0 6 F 13/00	6 1 0	G 0 6 F 13/00	6 1 0 Q

審査請求 未請求 請求項の数20 O L (全 15 頁)

(21) 出願番号 特願2002-46836(P2002-46836)

(22) 出願日 平成14年2月22日 (2002.2.22)

(71) 出願人 000232254

日本電気通信システム株式会社
東京都港区三田1丁目4番28号

(72) 発明者 白戸 寛之

東京都港区三田一丁目4番28号 日本電気
通信システム株式会社内

(74) 代理人 100084250

弁理士 丸山 隆夫

Fターム(参考) 5K030 GA11 HA06 LC15

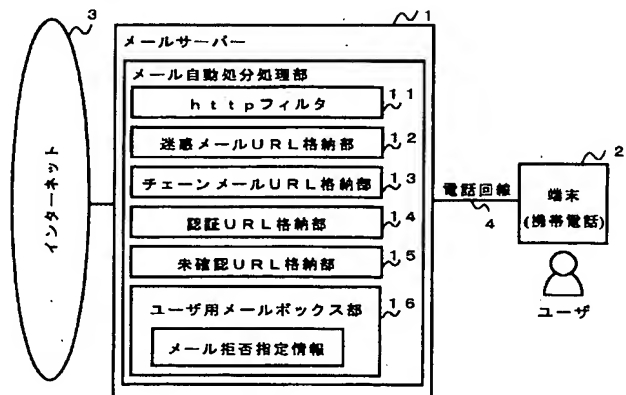
(54) 【発明の名称】 携帯電話のメールサーバーにおける迷惑メール自動処分方法及びプログラム

(57) 【要約】

【課題】 携帯電話のメールサーバーにおいて所定の識別条件により迷惑メール等を自動的に識別し、自動削除処理を行って余計な受信を防止すること。また、簡単なユーザ設定によりシステムを利用可能とすること。

【解決手段】 携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にURLが含まれるかどうかを調べ、含まれる場合は抽出する工程と、抽出されたURLを用いて受信メールが迷惑メールあるいはチェーンメールであるかの識別処理を行う工程と、識別処理の結果、迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する工程とを有する。上記識別条件は随時自動更新される。

システム構成



【特許請求の範囲】

【請求項1】 携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にURLが含まれるかどうかを調べ、含まれる場合は抽出する抽出工程と、該工程で抽出されたURLに基づき前記受信メールが迷惑メールあるいはチェーンメールであるか否かの識別処理を行う識別工程と、該工程で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する削除工程と、を有することを特徴とする迷惑メール自動処分方法。

【請求項2】 前記識別工程で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれていたURLを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する工程をさらに有することを特徴とする請求項1記載の迷惑メール自動処分方法。

【請求項3】 前記抽出工程で抽出されたURLが未確認URLである場合、該未確認URLを本文中に含む受信メールに対する所定時間の監視処理を開始し、該所定時間内は前記未確認URLを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、前記所定時間経過後、前記受信件数が所定件数を超える場合、前記未確認URLを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する監視工程をさらに有することを特徴とする請求項1または2に記載の迷惑メール自動処分方法。

【請求項4】 前記監視工程において、前記一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、前記未確認URLを本文中に含むメールは迷惑メールであると判定する工程をさらに有することを特徴とする請求項3記載の迷惑メール自動処分方法。

【請求項5】 前記監視工程において、前記一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、前記未確認URLを本文中に含むメールはチェーンメールであると判定する工程をさらに有することを特徴とする請求項3記載の迷惑メール自動処分方法。

【請求項6】 前記監視工程の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたURLを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する工程をさらに有することを特徴とする請求項3から5のいずれか1項に記載の迷惑メール自動処分方法。

【請求項7】 前記メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたURLを前記識別処理の際の識別条件となるURL情報として登録して管理し、前記識別工程では、

前記抽出工程で抽出されたURLについて、前記URL情報と比較し、一致する場合、前記受信メールを迷惑メールあるいはチェーンメールであると識別することの特徴とする請求項1から6のいずれか1項に記載の迷惑メール自動処分方法。

【請求項8】 前記メールサーバーにおいて、ユーザ設定情報として、前記識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、

前記受信メールについて迷惑メールあるいはチェーンメールと識別した場合、前記メール拒否指定の設定に基づき前記削除処理を実行することを特徴とする請求項1から7のいずれか1項に記載の迷惑メール自動処分方法。

【請求項9】 前記メールサーバーにおいて、前記メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、URLを本文中に含むメールに対する拒否指定であるURLメール拒否指定の3つの設定を保持し、該設定に基づき前記削除処理を実行することを特徴とする請求項8記載の迷惑メール自動処分方法。

【請求項10】 前記メールサーバーは、該メールサーバーの管理者により認証を受けたURLを登録して管理し、該URLを本文中に含む受信メールについては前記迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する工程を有することを特徴とする請求項1から9のいずれか1項に記載の迷惑メール自動処分方法。

【請求項11】 携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、

メール本文中にURLが含まれるかどうかを調べ、含まれる場合は抽出する抽出処理と、

該処理で抽出されたURLに基づき前記受信メールが迷惑メールあるいはチェーンメールであるか否かを識別する識別処理と、

該処理で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除する削除処理と、をコンピュータに実行させることを特徴とする迷惑メール自動処分プログラム。

【請求項12】 前記識別処理で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれるURLを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する処理をさらにコンピュータに実行させることを特徴とする請求項11記載の迷惑メール自動処分プログラム。

【請求項13】 前記抽出工程で抽出されたURLが未確認URLである場合、該未確認URLを本文中に含む受信メールに対する所定時間の監視処理を開始し、該所定時間内は、前記未確認URLを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、前

記所定時間経過後、前記受信件数が所定件数を超える場合、前記未確認URLを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する処理をコンピュータに実行させることを特徴とする請求項11または12に記載の迷惑メール自動処分プログラム。

【請求項14】 前記監視処理において、前記一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、前記未確認URLを含むメールは迷惑メールであると判定する処理をコンピュータに実行させることを特徴とする請求項13記載の迷惑メール自動処分プログラム。

【請求項15】 前記監視処理において、前記一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、前記未確認URLを含むメールはチェーンメールであると判定する処理をコンピュータに実行させることを特徴とする請求項13記載の迷惑メール自動処分プログラム。

【請求項16】 前記監視処理の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたURLを前記識別処理の際の識別条件として追加登録して該識別条件を自動更新する処理をコンピュータに実行させることを特徴とする請求項13から15のいずれか1項に記載の迷惑メール自動処分プログラム。

【請求項17】 前記メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたURLを前記識別処理の際の識別条件となるURL情報として登録して管理し、

前記識別処理では、

前記抽出処理で抽出されたURLについて、前記URL情報と比較し、一致する場合、前記受信メールを迷惑メールあるいはチェーンメールであると識別する処理をコンピュータに実行させることを特徴とする請求項11から16のいずれか1項に記載の迷惑メール自動処分プログラム。

【請求項18】 前記メールサーバーにおいて、ユーザ設定情報として、前記識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、前記受信メールについて迷惑メールあるいはチェーンメールと識別した場合、前記メール拒否指定の設定に基づき前記削除処理を行う処理をコンピュータに実行させることを特徴とする請求項11から17のいずれか1項に記載の迷惑メール自動処分プログラム。

【請求項19】 前記メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、URLを本文中に含むメールに対する拒否指定であるURLメール拒否指定の3つの設定を保持し、該設定に基づき前記削除処理を行う処理をコンピュータに実行させることを特徴とする請求項18記載の迷惑メール自動処分プログラム。

【請求項20】 前記メールサーバーにおいて、該メールサーバーの管理者により認証を受けたURLを登録管理し、該URLを本文中に含む受信メールについては前記迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する処理をコンピュータに実行させることを特徴とする請求項11から19のいずれか1項に記載の迷惑メール自動処分プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、携帯電話における電子メール技術に関し、特に、携帯電話のメールサーバーにおいて迷惑メール等を削除するメール自動処分方法及びプログラムに関する。

【0002】

【従来の技術】 昨今の電子メール機能を備える携帯電話機においては、迷惑メールによる被害が大きな問題になっている。被害として、ユーザの不快感や不要なパケット料金の支払いによる被害等が挙げられる。迷惑メールとしては様々な形態があり得るが、例えば、同一送信者からの大量のメールや、異なる送信者から同時に送信されてくるメール（チェーンメール）、あるいは、望まない広告や勧誘のメールなどがある。このようなメールに対する対策として、何らかの方法によりメールを自動的に排除・処分するシステムが求められている。

【0003】 従来の迷惑メール自動処分システムの一例として、特開2000-163341号公報に開示されている技術がある。以下、この技術を例に採って従来技術について説明する。図10は、この従来技術について説明するためのシステム構成図である。インターネット3には複数のメールサーバー1が接続されている。メールサーバー1には、電話回線4を通じて電子メール利用者（以下、ユーザ）の端末（携帯電話機）2が複数接続される。端末2は、電子メールの作成及び送受信機能を備える。電子メール（以下、「メール」）は、インターネット3を介してメールサーバー1間で送受信（配送、転送）処理される。メールサーバー1は、所定のメールサーバーソフトウェア（プログラム）を備える。

【0004】 メールサーバー1の各々は、個々のユーザに対するメール受信条件情報5を保持している。図11は、従来システムにおけるメールサーバー1での迷惑メール自動処分処理において用いられるメール受信条件情報5の構成図である。図11で、メール受信条件情報5には、ユーザのメール受信条件として、同一送信者条件51、最大サイズ条件52、既知送信者リスト53の情報が記述されている。

【0005】 同一送信者条件51は、同一のメール送信者から受信可能な（受信許可する）1日当たりのメール件数の上限値（例えば図10では、10件/日＝1日当たり10件まで）を表しており、同一のメール送信者から1日に大量の件数のメールを受信することを制限する

ために用いられる。

【0006】最大サイズ条件52は、メール1件当たりの受信可能なデータ量の上限値（例えば図10では、500KB/件＝1件当たり500KBまで）を表しており、非常に大きなサイズのメールを受信することを制限するために用いられる。

【0007】既知送信者リスト53は、ユーザが既知っている特定の個人（あるいはグループ）のメールアドレスが記述されるリストであり、ユーザが知らない個人（グループ）からのメール受信を制限するなどの目的で用いられる。例えば図11では、“aaa@xxx.co.jp”、“bbb@xxx.co.jp”等のメールアドレスがリストに登録されており、このアドレス情報を利用して受信メールについて所定の処理が行われる。

【0008】メール受信条件情報5における以上の各項目は、ユーザが任意に設定できる。メールサーバー1は、メール受信者（ユーザ）毎に以下のようなメール自動削除設定情報6をメール受信条件情報5内に保持する。なお、ユーザはメールアドレスで区別される。メール自動削除設定情報6は、メール受信者（ユーザ）により設定されるメール送信者毎のメール自動削除処理に関する設定項目の一覧を保持する。図12にメール自動削除設定情報6の構成を示す。

【0009】このメール自動削除設定情報6として、メール送信者毎に、送信者メールアドレス61、メール自動削除処理の対象とするか否かのオン/オフ設定62、メール自動削除処理の対象とする場合の1日当たりの受信可能（受信許可）メール件数上限値（以下、「受信上限値」）63、自動削除処理した場合に削除した旨の通知をメール送信者に対して行うか否かのオン/オフ設定（以下、「自動通知設定」）64、を有する。

【0010】また、ここで、メール送信者の要素に対する設定として、送信者不明メールについての設定65、送信者未知メール（不明ではないが既知送信者リスト53には記載されていない送信者からのメール）についての設定66も行えるものとする。

【0011】また、メール自動削除処理のための識別用の情報として、メール受信者（ユーザ）毎に、メール受信リスト67、ある1日におけるメール送信者毎のメール受信件数68を保持する。

【0012】次に、上記従来システムの動作を説明する。図13は、従来システムにおけるメールの送受信の様子を示す図である。例えば、同一のメール送信者7から、嫌がらせ等を目的とした大量のメールが送られてくる場合がある（俗にスパムメールと呼ばれる）。ただし、このようなメールの事例として、送信者メールアドレスが正規のものではない場合（ダミーのアドレスの場合）、あるいは、送信者メールアドレスが不明である場合なども含むとする。

【0013】図13で、メール送信者端末7からメールサーバー8を介して送出されるメールは、インターネット3を経由し、メール受信者（ユーザ）が利用するメールサーバー1に配送される。この際、メールサーバー1は、受信メールについて、ユーザにより予め設定されたメール受信条件情報5に基づき、この情報5内に記述されているメール受信条件を満足しないものを自動的に削除処理する。

【0014】ここで、「メール受信条件を満足しない」とは、次の3つの条件のうち最低1つを満足することを指している。

1：送信されてきたメールの件数が、同一送信者条件51で設定されている上限値を超えている。

2：送信されてきたメールのサイズが、最大サイズ条件52で設定される上限値を超えている。

3：送信されてきたメールの送信者メールアドレスが、既知送信者リスト53に記載されていない。

【0015】メールサーバー1における受信メールのうち、メール受信条件情報5内のメール受信条件を満足するメールについては、そのままメールサーバー1内のメールボックスに蓄積される。ユーザが端末2を使用して電話回線4を介してメールサーバー1に接続されている状態において、メールサーバー1に蓄積されている該当ユーザ宛のメールが端末2へ送信される（＝端末2におけるメール受信の完了）。

【0016】また、メールサーバー1は、メールを受信した際、受信メールから、メール受信者情報（宛先メールアドレス）、メール送信者情報（送信者メールアドレス）等を読む。続いて、該当メール受信者のメール自動削除設定情報6を参照しつつ、受信メールについて自動削除処理するか否かを識別・判定する。

【0017】メール自動削除設定情報6に基づく識別の結果、受信メールを自動削除しない場合、ユーザのメールボックスに蓄積する。メール受信者（ユーザ）によるメールサーバー1へのアクセスなどにより、メールボックスに蓄積されているメールがユーザの端末2に送信される。一方、上記識別の結果、受信メールを自動削除する場合、そのメールの送信者が既知メール送信者リスト53に記載されており、かつ自動通知設定64が「通知する」に設定されているならば、自動削除した旨およびその理由などを記載したメールを削除されたメールのメール送信者7宛に自動送信する。

【0018】次に、あるメール受信者（ユーザ）に関するメール自動削除設定情報6の例を説明する。例えば、不明送信者からのメールは1件たりとも受信しない設定にする場合、送信者メールアドレスが不明のメールに関して、自動削除機能62を「有効（する）」に設定し、受信上限値63を「0件」に設定し、自動通知機能64を「無効（しない）」に設定する。

【0019】また、未知送信者からのメールについて1

日当たり計20件まで受信可能とする設定にする場合、送信者メールアドレスが未知であるメールに関して、自動削除機能62を「有効」に設定し、受信上限値63を「20件」に設定し、自動通知機能64を「有効」に設定する。

【0020】また、送信者メールアドレスが“aaa@xxx.co.jp”のメールは1日当たり30件まで受信し、かつ自動削除した時に自動通知を行う設定にする場合、自動削除機能62を「有効」に設定し、受信上限値63を「30件」に設定し、自動通知機能64を

「有効」に設定する。

【0021】また、送信者メールアドレスが“bbb@xxx.co.jp”のメールは無制限に受信すると設定する場合、自動削除機能62を「無効」に設定し、受信上限値63を設定せず、自動通知機能64を「無効」に設定する。以上の各設定は、図14のようになる。

【0022】次に、上記のように自動削除設定した場合での、あるメール受信者（ユーザ）に関するメール受信リスト67の例を図15に示す。この例では、送信者アドレス“aaa@xxx.co.jp”からのメールは受信上限値63を30件に設定しているため、12件全てを受信している。また、送信者アドレス“bbb@xxx.co.jp”からのメールは受信上限値63が設定されていないため、32件全てを受信している。これに対し、送信者アドレス“ccc～”、“ddd～”、“eee～”（いずれも未知送信者）からのメールについては、メール受信件数の合計が未知送信者メールの設定66での受信上限値（この場合は20件）に達したため、これ以降の未知送信者からのメールは自動削除の対象となったという状態を示している。

【0023】メールサーバー1が以上のような設定及び処理により動作することにより、メール受信者（ユーザ）が不要と考える性質のメールについて、メール受信条件の設定により識別し、受信（つまりメールサーバー1における蓄積及び端末2への送信）を行わない。これにより、不要なメールのための無駄な電話回線4の使用及び端末2へのメール受信を回避できる。メール受信者（ユーザ）は、同一のメール送信者から設定上限値を超える件数のメールを受信することがない。スパムメールのような、何千、何万といった件数になるようなメールはメールサーバー1において未然に削除されるため、メール受信者（ユーザ）の端末2が電話回線4でメールサーバー1につなぎっぱなしになってしまうというような被害を回避できる。

【0024】また、メール自動削除設定情報6をメール受信者（ユーザ）が任意に設定することにより、メール送信者毎の細かな自動削除／受信許可の指定を行うことができる。未知のメール送信者、あるいは不明のメール送信者からのメールについても、自動削除／受信許可を指定できる。また、例えば、メール自動削除設定情報6

において特定の送信者メールアドレスを記載し、自動削除機能を有効に設定にし、受信上限値を0件とすることで、この特定の送信者からのメールを一切受け取らないようにするといったこともできる。

【0025】更に、メールサーバー1は、受信メールを自動削除処理した場合、メール自動削除設定情報6の自動通知設定64に基づき、削除されたメールの送信者に対して、自動削除処理した旨及び自動削除の理由などを記載したメールを自動送信する。これにより、メール送信者は、自分のメールが受信者に届かなかったことを知ることができる。

【0026】なお、この従来技術はメールサーバー1（特にソフトウェア）のみの改良により効果を発揮できるものなので、ユーザの端末2（メール送受信ソフトウェアを含む）を改変する必要はない。

【0027】

【発明が解決しようとする課題】しかしながら、上記従来技術では以下のような問題点がある。第1の問題点として、メール受信者（ユーザ）が既知の個人（グループ）に関するメール受信設定を行うために、ユーザ自身がメールサーバーに送信者メールアドレス他の情報を登録処理する必要があるという点が挙げられる。ユーザによる登録処理により、必要時にすぐにメールアドレスを設定して受信を限定するなどができる。しかし、メールアドレスの登録処理には基本的に手間がかかる。また、現在の携帯電話は、上記受信設定として登録可能な件数が少なく、足りなくなることが多い。また、仮にたくさんの件数を登録可能だとしても、すべてのメールアドレス情報などを登録するための大きな手間が生じる。

【0028】第2の問題点として、メール受信条件として同一送信者から1日に受信可能な件数の上限を設定して受信制限を行う機能の場合、例えば1日に受信する件数を1～3件のように少ない件数に設定しても、結局はその件数分が届けられてしまうことが多く、逆に件数を多く設定すると迷惑メールを防ぐことにならないなど、効果的な件数設定の仕方が難しいという点が挙げられる。

【0029】第3の問題点として、メール受信条件としてユーザがメールアドレスを知らない未知の個人（グループ）からのメール受信を制限する機能の場合、未知のメールアドレスであっても知人や友人などからの可能性のあるメールについて制限してしまう点が挙げられる。

【0030】本発明は、かかる問題点を鑑みてなされたものであり、携帯電話のメールサーバーにおいて所定の識別条件により迷惑メール等を自動的に識別し、また、迷惑メール等について送信者メールアドレスなどの情報が変更されても上記識別条件を自動更新して識別を行い、迷惑メール等の自動削除処理を行って余計な受信を防止することのできる携帯電話のメールサーバーにおけるメール自動処分方法及びプログラムを提供することを

目的とする。

【0031】また、ユーザが受信条件としてメールアドレスの登録処理を行うといった面倒な手間を必要とせずに、わずかな初期設定のみでシステムを利用できるメールサーバーにおけるメール自動処分方法及びプログラムを提供することを目的とする。

【0032】

【課題を解決するための手段】かかる目的を達成するために、請求項1記載の発明は、携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にURLが含まれるかどうかを調べ、含まれる場合は抽出する抽出工程と、該工程で抽出されたURLに基づき受信メールが迷惑メールあるいはチェーンメールであるか否かの識別処理を行う識別工程と、該工程で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除処理する削除工程と、を有することを特徴としている。

【0033】請求項2記載の発明は、請求項1記載の発明において、識別工程で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれていたURLを識別処理の際の識別条件として追加登録して識別条件を自動更新する工程をさらに有することを特徴としている。

【0034】請求項3記載の発明は、請求項1または2に記載の発明において、抽出工程で抽出されたURLが未確認URLである場合、該未確認URLを本文中に含む受信メールに対する所定時間の監視処理を開始し、所定時間内は未確認URLを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、所定時間経過後、受信件数が所定件数を超える場合、未確認URLを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する監視工程をさらに有することを特徴としている。

【0035】請求項4記載の発明は、請求項3記載の発明において、監視工程において、一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、未確認URLを本文中に含むメールは迷惑メールであると判定する工程をさらに有することを特徴としている。

【0036】請求項5記載の発明は、請求項3記載の発明において、監視工程において、一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、未確認URLを本文中に含むメールはチェーンメールであると判定する工程をさらに有することを特徴としている。

【0037】請求項6記載の発明は、請求項3から5のいずれか1項に記載の発明において、監視工程の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたURLを識別処理の際の識別条件と

して追加登録して識別条件を自動更新する工程をさらに有することを特徴としている。

【0038】請求項7記載の発明は、請求項1から6のいずれか1項に記載の発明において、メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたURLを識別処理の際の識別条件となるURL情報として登録して管理し、識別工程では、抽出工程で抽出されたURLについて、URL情報と比較し、一致する場合、受信メールを迷惑メールあるいはチェーンメールであると識別することを特徴としている。

【0039】請求項8記載の発明は、請求項1から7のいずれか1項に記載の発明において、メールサーバーにおいて、ユーザ設定情報として、識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、受信メールについて迷惑メールあるいはチェーンメールと識別した場合、メール拒否指定の設定に基づき削除処理を実行することを特徴としている。

【0040】請求項9記載の発明は、請求項8記載の発明において、メールサーバーにおいて、メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、URLを本文中に含むメールに対する拒否指定であるURLメール拒否指定の3つの設定を保持し、該設定に基づき削除処理を実行することを特徴としている。

【0041】請求項10記載の発明は、請求項1から9のいずれか1項に記載の発明において、メールサーバーは、メールサーバーの管理者により認証を受けたURLを登録して管理し、該URLを本文中に含む受信メールについては迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する工程を有することを特徴としている。

【0042】請求項11記載の発明は、携帯電話のメールサーバーにおいて、ネットワーク経由で受信したメールについて、メール本文中にURLが含まれるかどうかを調べ、含まれる場合は抽出する抽出処理と、該処理で抽出されたURLに基づき受信メールが迷惑メールあるいはチェーンメールであるか否かを識別する識別処理と、該処理で迷惑メールあるいはチェーンメールであると識別された受信メールについてユーザ宛のメールボックスに蓄積せずに削除する削除処理と、をコンピュータに実行させることを特徴としている。

【0043】請求項12記載の発明は、請求項11記載の発明において、識別処理で迷惑メールあるいはチェーンメールであると識別された受信メールに含まれるURLを識別処理の際の識別条件として追加登録して識別条件を自動更新する処理をさらにコンピュータに実行させることを特徴としている。

【0044】請求項13記載の発明は、請求項11また

は12に記載の発明において、抽出工程で抽出されたURLが未確認URLである場合、該未確認URLを本文中に含む受信メールに対する所定時間の監視処理を開始し、所定時間内は、未確認URLを本文中に含む受信メールを一時格納領域に格納して受信件数をカウントし、所定時間経過後、受信件数が所定件数を超える場合、未確認URLを本文中に含むメールを迷惑メールまたはチェーンメールであると判定する処理をコンピュータに実行させることを特徴としている。

【0045】請求項14記載の発明は、請求項13記載の発明において、監視処理において、一時格納領域に格納した受信メールが同一送信者からの所定受信件数を超えるメールである場合、未確認URLを含むメールは迷惑メールであると判定する処理をコンピュータに実行させることを特徴としている。

【0046】請求項15記載の発明は、請求項13記載の発明において、監視処理において、一時格納領域に格納した受信メールが異なる送信者からの所定受信件数を超えるメールである場合、未確認URLを含むメールはチェーンメールであると判定する処理をコンピュータに実行させることを特徴としている。

【0047】請求項16記載の発明は、請求項13から15のいずれか1項に記載の発明において、監視処理の結果、迷惑メールまたはチェーンメールであると判定されたメールに含まれていたURLを識別処理の際の識別条件として追加登録して識別条件を自動更新する処理をコンピュータに実行させることを特徴としている。

【0048】請求項17記載の発明は、請求項11から16のいずれか1項に記載の発明において、メールサーバーは、過去に迷惑メールあるいはチェーンメールであると識別されたメールに含まれていたURLを識別処理の際の識別条件となるURL情報として登録して管理し、識別処理では、抽出処理で抽出されたURLについて、URL情報と比較し、一致する場合、受信メールを迷惑メールあるいはチェーンメールであると識別する処理をコンピュータに実行させることを特徴としている。

【0049】請求項18記載の発明は、請求項11から17のいずれか1項に記載の発明において、メールサーバーにおいて、ユーザ設定情報として、識別処理の結果に基づく迷惑メールあるいはチェーンメールの削除処理を有効とするか否かのメール拒否指定の設定を保持し、受信メールについて迷惑メールあるいはチェーンメールと識別した場合、メール拒否指定の設定に基づき削除処理を行う処理をコンピュータに実行させることを特徴としている。

【0050】請求項19記載の発明は、請求項18記載の発明において、メール拒否指定の設定として、迷惑メール拒否指定、チェーンメール拒否指定、及び、URLを本文中に含むメールに対する拒否指定であるURLメール拒否指定の3つの設定を保持し、該設定に基づき削

除処理を行う処理をコンピュータに実行させることを特徴としている。

【0051】請求項20記載の発明は、請求項11から19のいずれか1項に記載の発明において、メールサーバーにおいて、メールサーバーの管理者により認証を受けたURLを登録管理し、該URLを本文中に含む受信メールについては迷惑メールあるいはチェーンメールと区別してユーザ宛のメールボックスに格納する処理をコンピュータに実行させることを特徴としている。

【0052】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。図1は、本発明の実施の形態におけるメール自動処分方法及びプログラムが実行されるシステムの構成図である。本システムは、メールサーバー1、ユーザの使用する携帯電話端末2、インターネット3、電話回線4、を有する。基本的なシステム構成は従来技術と同様であり、同一の記号によって示した。

【0053】メールサーバー1は、本発明の実施の形態におけるメール自動処分方法を実行するサーバー装置であり、このメール自動処分方法をコンピュータ処理により実現するためのプログラム(図1でのメール自動処分処理部)を含むメールサーバーソフトウェアがインストールされ、プロセッサにより実行される。インターネット3には、複数のメールサーバー1が接続され、メールの送受信処理を行う。メールサーバー1には、電話回線4を通じて複数の端末2が接続される。ここで端末2は特に携帯電話機であるので、電話回線4は、無線通信網を含む所定の通信システムで構成される。端末2は、メールを作成・送受信する機能を持つメールソフトウェアを備える。端末2がメールサーバー1に接続された状態において、端末2はメールサーバー1に蓄積されているユーザ宛のメールを取得することができる。

【0054】図1で、メールサーバー1の備えるプログラムは、構成要素として、httpフィルタ11、迷惑メールURL格納部12、チェーンメールURL格納部13、認証URL格納部14、未確認URL格納部15、ユーザ用メールボックス部16を有する。メールサーバー1は、所定のメール配送処理他の公知処理を行う。

【0055】各格納部12～16は、メールサーバー1の備える記憶装置(非図示)のメモリ領域への情報の格納処理を行うモジュールであり、メモリ上に確保される各情報欄やメールボックスを管理する(後述)。ユーザ用メールボックス部16は、ユーザ宛のメールを蓄積するメールボックスを管理し、また、当該メールシステムを利用するに当たってのユーザによる初期設定情報であるメール拒否指定情報を管理する。

【0056】本明細書において、迷惑メールとは、同一送信者からの多数のメールを指す。チェーンメールと

は、異なる多数の送信者から送信されてくる同一内容のメールを指す。

【0057】本方法は、メールサーバー1がユーザ宛の受信メールについてメール本文中に書かれているホームページアドレス（URL）をチェック対象とすることを特徴としている。ホームページアドレス（Webページアドレス）はURLにより記述される。URL（Uniform Resource Locator）とは、ネットワーク上におけるリソース指示子である。これは、例えば、“http://www.xyz.com”などの形式で記述される。“http:”は、リソースへのアクセスに用いるプロトコルの指定であり、この場合httpプロトコルを用いている。“www.～”は、ネットワーク上におけるリソースのアドレス（及びパス）の一意指定である。

【0058】本方法において、メールサーバー1は、上記のURLチェック処理を行うhttpフィルタ11を備える。httpフィルタ11は、インターネット3を介してメールサーバー1が受信したメールについて、メール本文にURLが含まれているかどうかを調べ、含まれている場合はURL文字列を情報として抽出する処理を行う（なお、この処理は文字列自体を抜き出す処理ではない）。本方法では、受信メール本文中から抽出したURLを識別の条件として用いて迷惑メールやチェーンメールであるかどうかを識別し、この識別の結果に応じてメールを自動処分処理するものである。

【0059】本方法では、メールサーバー1に、httpフィルタ11によりメール本文中から抽出されたURLを格納処理する迷惑メールURL格納部12、チェーンメールURL格納部13他を設ける。各格納部12、13他は、抽出されたURLを使用して、受信メールが迷惑メールあるいはチェーンメールかどうかの識別処理を行う。この識別処理によって迷惑メールあるいはチェーンメールであると識別されたメールに書かれていた該当URLは、迷惑メールURL格納部12、チェーンメールURL格納部13において保存・管理され、以後の受信メールに対する迷惑メール等であるかどうかの識別条件として使用される。この識別条件は、メール受信に伴い、随時更新される。

【0060】メールサーバー1の各格納部12、13他は、受信メールについて、識別条件として格納されているURLと比較する処理を行うことにより、そのメールが迷惑メールあるいはチェーンメールあるいはその他のメールであるかを識別する。

【0061】メールサーバー1は、メール受信時、ユーザによる受信メールについての拒否指定情報（後述）に基づき、その拒否指定で設定される拒否条件に該当する受信メールをユーザ用メールボックス部16内のメールボックスに格納保存せず、自動削除処理する。

【0062】このように、本方法では、受信メールについてURLを参照して迷惑メール・チェーンメール等の

識別を行って該当メールを自動削除処理することによって、同一送信者から1日に受信可能なメール件数などの従来のような設定処理をする必要なくメール受信制限処理を実現する。また既知送信者以外からのメール受信の制限のための設定処理を行う必要もない。

【0063】本方法では、ユーザ（メール受信者）は、迷惑メールやチェーンメールの受信を拒否したい場合、メールサーバー1に上述したメール拒否指定を設定する。メールサーバー1において、上記メール拒否指定の設定及びユーザ宛に届くメールは、各ユーザ毎のユーザ用メールボックス部16内に保存・管理される。

【0064】図6は、ユーザ用メールボックス部16の管理する情報を示す図である。ユーザ用メールボックス部16は、ユーザ宛のメールをユーザ端末2に送信するまで蓄積しておくメールボックスである送信ボックス161と、迷惑メールやチェーンメールやメール本文中にURLの書かれたメール（以下、「URLメール」）に対する拒否指定の設定情報であるメール拒否指定情報とを管理する。メール拒否指定情報として、迷惑メール拒否指定欄162、チェーンメール拒否指定欄163、URLメール拒否指定欄164を設ける。本方法では、この3つの設定欄と送信ボックスを要素とするユーザ用メールボックス部16を設けたことも特徴としている。

【0065】URLメール拒否指定は、メール本文中にURLを含むメールに対する拒否であるので、これにより、迷惑メール及びチェーンメールの拒否を含む拒否指定を行うことができる。

【0066】図7は、ユーザの端末2における、上記拒否指定を設定するための設定画面の例を示す。図7では、迷惑メール、チェーンメール、及び、URLメールの各メールに対する拒否指定として、YES/NOの項目をチェックすることにより設定登録が行われる。このような設定画面を介してユーザ用メールボックス部16における各拒否指定欄162～164への設定処理が行われる。本方法では、ユーザは上記の3項目の設定のみにより迷惑メール等自動削除処理を有効とするための拒否指定の設定を行うことができる。

【0067】図2は、迷惑メールURL格納部12の管理する迷惑メールURL格納欄の構成を示す。迷惑メールURL格納欄はいくつかのURL格納欄から成り立っている。迷惑メールURL格納欄には過去に当該メールサーバー1において迷惑メールであると識別されたメールに書かれていたURL（以下、「迷惑メールURL」）が格納される。

【0068】図3は、チェーンメールURL格納部13の管理するチェーンメールURL格納欄の構成を示す。チェーンメールURL格納欄はいくつかの格納欄から成り立っている。チェーンメールURL格納欄には過去に当該メールサーバー1においてチェーンメールと識別されたメールに書かれていたURL（以下、「チェーンメ

ールURL」)が格納される。

【0069】メールサーバー1が受信するメールでメール本文中にURLが書かれているメールとしては、迷惑メールやチェーンメールだけではないと考えられる。例えば、メーカーやメールサーバー1の管理者からの連絡などのメールにもURLが書かれている場合がある。本方法では、メールサーバー1は、メールサーバー1の管理者等により認証を受けたURL(以下、「認証URL」)を保存・管理する領域である認証URL格納部14を設ける。認証URL格納部14では、迷惑メール等に含まれるURL以外の、メールサーバー1管理者により認証を受けたURLを格納する。この格納部14により、メーカーやメールサーバー1の管理者からの連絡などのメールでURLを含むものについて、迷惑メールやチェーンメールなどと区別して受信許可することができ、このようなメールをユーザが通常通り受信することが可能となる。

【0070】メールサーバー1は、受信メールについて、認証URL格納部14の管理する認証URLを参照し、認証URLが書かれているメールについては迷惑メール等ではないと識別してユーザ用メールボックス部16への格納を行う。本方法は、この認証URLを用いた処理を行うことも特徴としている。

【0071】次に、本方法ではまた、メールサーバー1は、受信メールについて未確認URLの記載を発見した場合にこのURLを格納し、以後の受信メールについて監視してこの未確認URLが記載されたメールが迷惑メール等かどうかの識別処理を行う未確認URL格納部15を設ける。ここで未確認URLとは、メール受信時点で、メールサーバー1において迷惑メールURLやチェーンメールURLあるいは認証URL等の情報としては登録されていないURLを指す。未確認URL格納部15は、図5に参照されるような未確認URL確認欄を管理する。

【0072】メールサーバー1のhttpフィルタ11及び未確認URL格納部15は、受信メールの本文中に新しく未確認のURLを発見した場合、一旦この未確認URLを未確認URL格納欄に格納し、また、この未確認URLを含む受信メールを一時格納領域を確保して格納し、この時点以後の所定の一定時間、受信メールについて、上記未確認URLが記載されたメールかどうかを監視処理することにより、この未確認URLが記載されたメールが迷惑メールあるいはチェーンメールあるいはそうではない普通のメールかどうかの識別処理を行う。識別処理の結果、迷惑メールと識別した場合は、迷惑メールURL格納部12の格納欄に格納し、チェーンメールと識別した場合はチェーンメールURL格納部13の格納欄に格納し、普通のメールと識別した場合はユーザ用メールボックス部16の送信ボックス161に格納する。これらにより、未確認のURLが記載されているメ

ールに自動的に対処する。監視処理の結果、迷惑メールあるいはチェーンメールと識別されたメールについては、メール拒否指定の設定に基づき、一時格納領域に格納されている受信メールを削除処理する。

【0073】図5は、未確認URL確認欄の構成を示す。未確認URLごとに、情報領域が確保される。未確認URLごとに、そのURL文字列151、送信者メールアドレス152、アクセス数153などの情報を管理する。未確認URL格納部15は、受信メールで未確認URLが記載されたものを発見した場合、このような情報領域を確保して、その時点以後、所定の一定時間、監視処理を行う。監視処理では、一定時間内において、該当未確認URLと同じURLが本文中に記載されたメールを受信した場合、受信メールを一時格納領域に格納して、未確認URL格納欄中の該当の未確認URL151の情報を更新する。その際、受信メールについて送信者メールアドレスを参照し、その送信者メールアドレス152ごとにレコードを設けてメール受信件数であるアクセス数153をカウントする。また、異なる未確認URLを新たに抽出した場合は、次の未確認URL151情報欄を設けて格納し監視処理する。

【0074】例えば、図5では、未確認URL1“www.abc.co.jp”を含んだメールとして、所定の一定時間内に、送信者“aaa@bbb.com”から28件のメールを受信し、送信者“ccc@ddd.co.jp”から12件のメールを受信したことを示している。

【0075】未確認URL格納部15は、上記監視処理で所定の一定時間経過後、該当未確認URLの管理情報を参照して該当未確認URLを含むメールが迷惑メールあるいはチェーンメールであるかどうか判定を行う。ある未確認URLについて、ある送信者メールアドレス152でアクセス数153が所定の件数を超える場合、迷惑メールであると判定する。また、複数の送信者メールアドレス152があり、それらを合わせたアクセス数153が所定の件数を超える場合、チェーンメールであると判定する。

【0076】メールサーバー1は、上記の処理で迷惑メールあるいはチェーンメールの含むURLであると判定された未確認URLについて、今度は、それぞれ迷惑メールURLあるいはチェーンメールURLとして、格納部12、13の格納欄へそれぞれ格納し、迷惑メールあるいはチェーンメールの識別処理の際の識別条件となるURL情報として追加登録する。各格納部12、13は、追加登録されたURL情報を用いて識別処理の際の識別条件を更新し、更新された識別条件を用いてその後の識別処理を行う。

【0077】次に、図8及び図9のフローチャートを参照して、本発明の実施の形態におけるメール自動処分方法及びプログラムを実行するメールサーバー1の動作について説明する。以下の処理の主体はメールサーバー1

である。図8で、まず、メールサーバー1は、ユーザ宛のメールをインターネット3経由で受信した場合、受信メールをhttpフィルタ11に通し(ステップS101)、メール本文中にURL(ホームページアドレス)が書かれているかどうかを調べる(ステップS102)。具体的には、まず"http"という文字列を検出し、メール本文中に"http"文字列が含まれる場合、その"http"文字列を含んで以後に続く文字列からなるURL文字列について、ステップS104以後の確認処理を順に行う。URL文字列を含まないメールである場合、受信メールをユーザ用メールボックス部16の送信ボックス161に格納する(ステップS103)。

【0078】URL文字列をメール本文に含む受信メールについて、まず、迷惑メールURL格納部12に格納されている迷惑メールURLで一致するものがないか比較して確認する(ステップS104)。

【0079】一致するURLがある場合(ステップS105・YES)、当該受信メールを迷惑メールであると判定し、次に、ユーザ用メールボックス部16の迷惑メール拒否指定欄162及びURLメール拒否指定欄164の各拒否指定を確認し(ステップS106、S109)、拒否指定がなければ、送信ボックス161へ格納する(ステップS112)。拒否指定がある場合、各部は、当該受信メールについて、自動的な削除処理を行う(ステップS108、S111)。

【0080】一致するURLはない場合(ステップS105・NO)、次に、チェーンメールURL格納部13に格納されているチェーンメールURLで一致するものがないか比較して確認する(ステップS113、14)。

【0081】一致するURLがある場合(ステップS114・YES)、当該受信メールをチェーンメールであると判定し、ユーザ用メールボックス部16のチェーンメール拒否指定欄163及びURLメール拒否指定欄164の各拒否指定を確認し(ステップS115、S118)、拒否指定がなければ、送信ボックス161へ格納する(ステップS121)。拒否指定がある場合、当該受信メールについて自動的な削除処理を行う(ステップS117、S120)。

【0082】一致するURLがない場合(ステップS114・NO、図8へ)、次に、認証URL格納部15に格納されている認証URLで一致するものがないかを比較して確認する(図9、ステップS201)。

【0083】一致するURLがある場合(ステップS202・YES)、当該URLを認証URLであると判定し、送信ボックス161へ格納する(ステップS203)。

【0084】一致するURLはない場合(ステップS202・NO)、当該URLは未確認URLであると判定

し、未確認URL格納部15の格納欄中にこの未確認URL用の情報領域を確保して格納する(ステップS204)。そして、この未確認URLに関して、所定の一定時間の監視処理を行う(ステップS205)。この監視処理では、所定の一定時間内に当該未確認URLと同じURLを本文中に含むメールを受信した場合に、上記確保された未確認URL情報領域の情報(送信者メールアドレス152、アクセス数153など)を更新する。また、別の未確認URLが含まれたメールを受信した場合には、未確認URL格納欄中に別の情報領域を確保して独立した所定の一定時間の監視処理を開始する。この監視処理において、監視対象である各未確認URLを含む受信メールについては、上記一定時間内は未確認URL格納部15が確保する一時格納領域において一時蓄積する。

【0085】未確認URLに関して上記一定時間監視後、未確認URL格納欄中のアクセス数153等を参照し、アクセス数153が所定数を超える場合(ステップS206・YES)、この未確認URLを含むメールは迷惑メールもしくはチェーンメールのどちらかであると識別する。

【0086】上記のように識別された未確認URLを含む受信メールについて、未格納URL確認欄中の送信者メールアドレス152やアクセス数153を参照し、同一送信者からの所定数以上のメールである場合、このURLを含むメールを迷惑メールであると判定し、このURLを迷惑メールURLとして迷惑メールURL格納部12に新たに登録する(ステップS209)。

【0087】また、異なる送信者からの所定数以上のメールである場合、このURLを含むメールをチェーンメールであると判定し、このURLをチェーンメールURLとしてチェーンメールURL格納部13に新たに登録する(ステップS212)。

【0088】迷惑メールと判定した場合、ユーザ用メールボックス部16の迷惑メール拒否指定欄162及びURLメール拒否指定欄164の拒否指定を確認し(ステップS210、S215)、拒否指定があれば該当受信メールを自動削除し(ステップS211、S217)、拒否指定がなければ送信ボックス161に格納する(ステップS218)。

【0089】同様に、チェーンメールと判定した場合、ユーザ用メールボックス部16のチェーンメール拒否指定欄163及びURLメール拒否指定欄164を確認し(ステップS213、S216)、拒否指定があれば該当受信メールを自動削除し(ステップS214、S217)、なければ送信ボックス161に格納する(ステップS218)。動作については以上である。

【0090】以上により本発明の実施の形態について説明した。なお、上述した実施形態は、本発明の好適な実施形態の一例を示すものであり、本発明はそれに限定さ

れるものではなく、その要旨を逸脱しない範囲内において、種々変形実施が可能である。

【0091】

【発明の効果】以上の説明から明らかなように、本発明によれば、携帯電話のメールサーバーにおいて受信メール本文中にURLが書かれているかどうか調べ、このURLを識別条件として用いて迷惑メール等であるか否かの識別を行うので、URL（ホームページアドレス）が本文中に書かれたメール（例えば、広告や勧誘としてURLを記載しているもの）について自動的に迷惑メール等の識別を行って自動処分し、ユーザの端末への受信を防止することができる。

【0092】また、メールサーバーにおいて過去に迷惑メール等に含まれるURLであると判定されたURLを保存・管理し、これを用いて受信メールについて識別を行うことにより、瞬時にその受信メールが迷惑メール等であるかを識別することができる。

【0093】また、この迷惑メール等識別処理のためのURL情報はメールサーバーにおいて自動的に更新されるため、ユーザが細かな設定や再登録処理を行う必要がない。

【0094】また、ユーザが当該メールシステムを利用するに当たって初期設定処理として必要なのは拒否指定欄における3つの設定であって手間が少なく、ユーザは面倒な登録処理をする必要がない。

【0095】また、認証URL格納部を設けたことにより、メールサーバー管理者やメーカー等からの連絡のメールの本文中にURLが書かれていても、迷惑メール等との区別ができ、このようなメールについて削除処理してしまうことなく必要としているユーザに届けることができる。

【0096】また、未確認URL格納部を設けたことにより、受信メールの本文中に未確認のURLが書かれていても、そのURLに関して迷惑メール等であるかの識別ができ、自動処分や蓄積等の対応処理を行うことができる。迷惑メール等の送信者が送信元メールアドレスを変更したり、本文中のURLを変更したメールを送信してくる場合にも対応できる。

【図面の簡単な説明】

【図1】本発明の実施の形態における迷惑メール自動処分方法及びプログラムを実行するシステムの基本構成図である。

【図2】迷惑メールURL格納欄の構成図である。

【図3】チェーンメールURL格納欄の構成図である。

【図4】認証URL格納欄の構成図である。

【図5】未確認URL格納欄の構成図である。

【図6】ユーザ用メールボックス部16の管理情報の構成図である。

【図7】ユーザの端末2における、各拒否指定の設定画面の例である。

【図8】本発明の実施の形態における迷惑メール自動処分方法及びプログラムの動作を示すフローチャートである。

【図9】本発明の実施の形態における迷惑メール自動処分方法及びプログラムの動作を示すフローチャート（図8の続き）である。

【図10】従来技術のシステムの基本構成図である。

【図11】従来技術のメールサーバー1における迷惑メール自動処分方法で用いられるメール受信条件情報5の構成図である。

【図12】従来技術のメールサーバー1におけるメール自動削除設定情報6の構成図である。

【図13】従来技術のシステムにおけるメールの送受信の様子を示す図である。

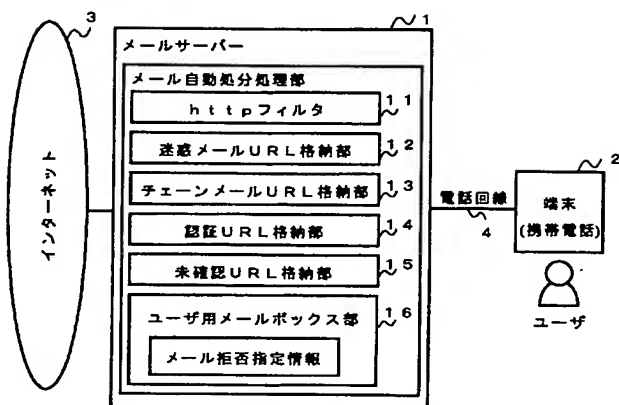
【図14】メール自動削除の設定例である。

【図15】メール受信リスト67の例である。

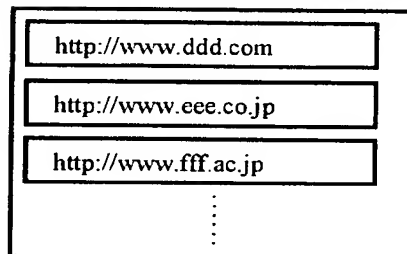
【符号の説明】

- 1 メールサーバー
- 2 ユーザの携帯電話端末
- 3 インターネット
- 4 電話回線
- 11 httpフィルタ
- 12 迷惑メールURL格納部
- 13 チェーンメールURL格納部
- 14 認証URL格納部
- 15 未確認URL格納部
- 16 ユーザ用メールボックス部
- 151 未確認URL
- 152 送信者メールアドレス
- 153 アクセス数
- 161 送信ボックス
- 162 迷惑メール拒否指定欄
- 163 チェーンメール拒否指定欄
- 164 URLメール拒否指定欄
- 5 メール受信条件情報（従来技術）
- 6 メール自動削除設定情報（従来技術）
- 7 メール送信者及び送信者端末
- 8 送信側メールサーバー
- 51 同一送信者条件
- 52 最大サイズ条件
- 53 既知送信者リスト
- 61 送信者メールアドレス
- 62 自動削除対象の設定情報
- 63 受信可能メール件数の上限値
- 64 削除通知設定
- 65 送信者不明メールの設定
- 66 送信者未知メールの設定
- 67 メール受信リスト
- 68 日単位・送信者単位でのメール受信件数

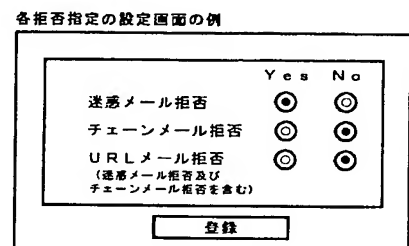
【図 2】



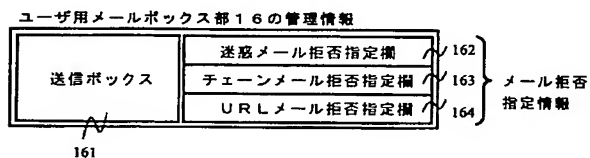
【図 4】



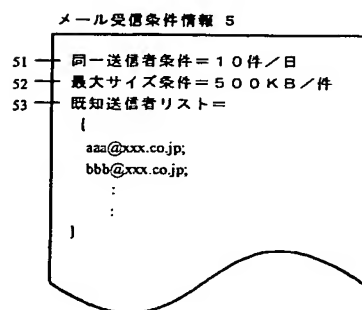
【图 7】



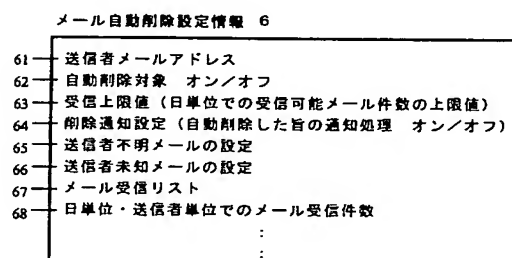
【图 10】



【图 1 1】



【図 1 2】



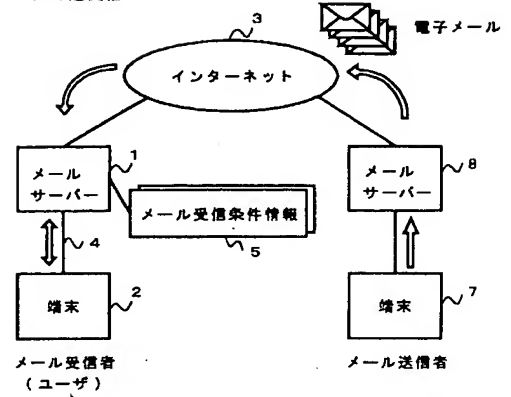
【図5】

未確認URL格納欄

未確認URL 1		http://www.abc.co.jp	151
152	送信者メールアドレス	アクセス数	153
	aaa@bbb.com	28	
	ccc@ddd.co.jp	12	
	
未確認URL 2		http://www.def.com	
	送信者メールアドレス	アクセス数	
	xxx@yyy.com	10	
	zzz@uuu.co.jp	36	
	www@aaa.com	3	
	

【図13】

メールの送受信



【図14】

メール自動削除の設定例

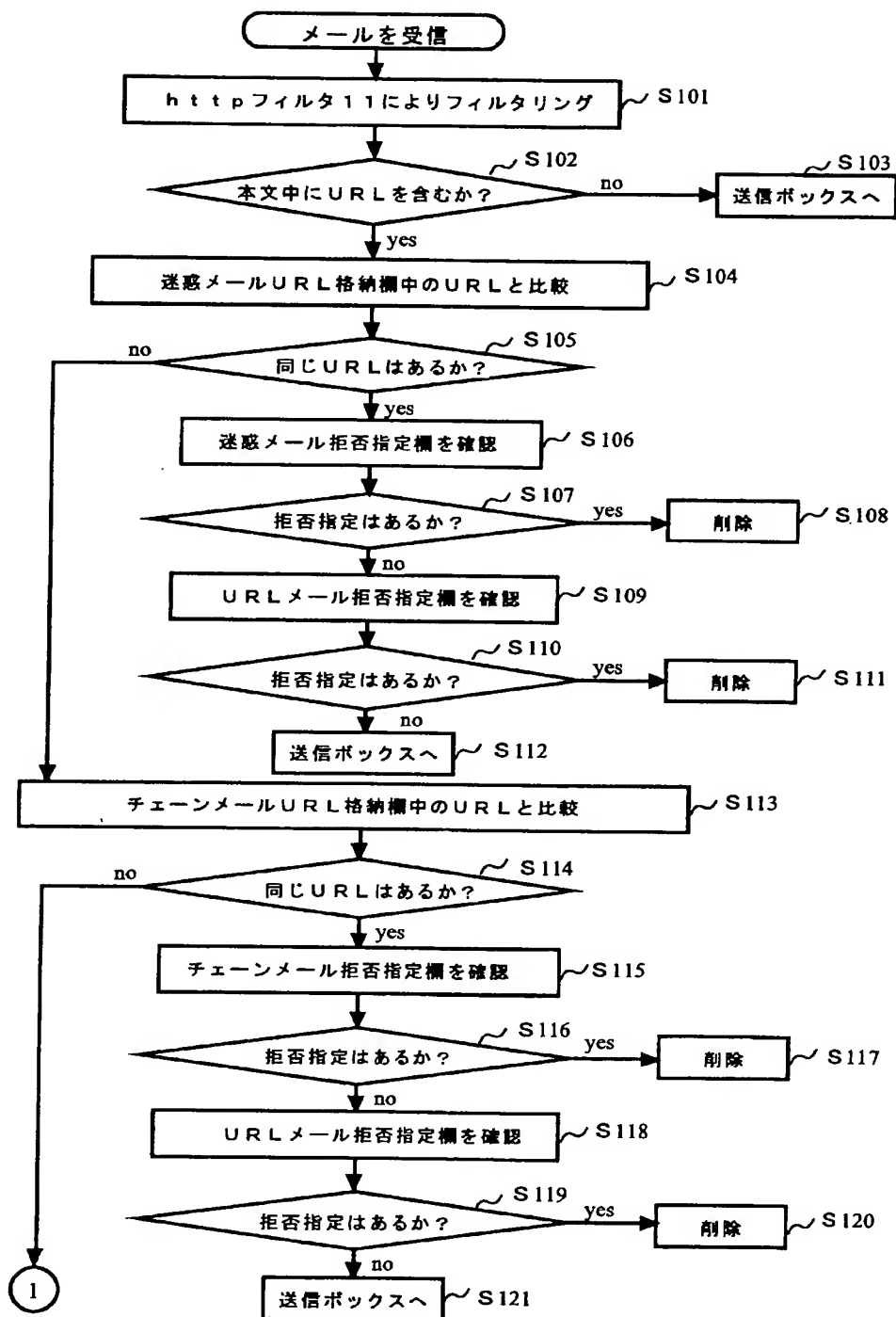
送信者メールアドレス	自動削除	受信上限値	自動通知
不明送信者	する	0件	しない
未知送信者	する	20件	する
aaa@xxx.co.jp	する	30件	する
bbb@xxx.co.jp	しない	—	—

【図15】

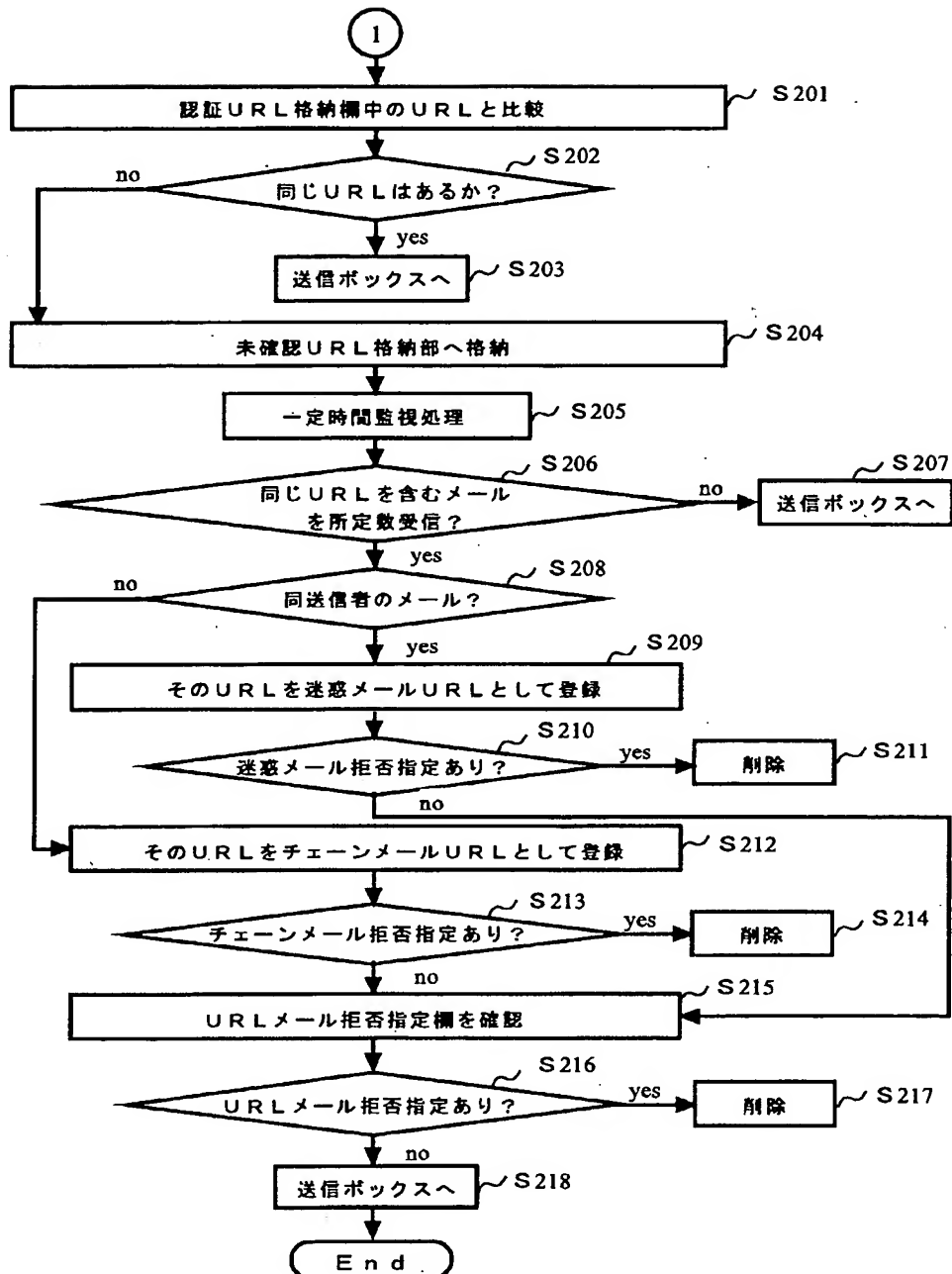
メール受信リスト67の例

送信者メールアドレス	本日の件数	(備考)
不明送信者	0件	
aaa@xxx.co.jp	12件	
bbb@xxx.co.jp	32件	
ccc@xxx.co.jp	8件	(未知送信者)
ddd@xxx.co.jp	10件	(未知送信者)
eee@xxx.co.jp	2件	(未知送信者)

【図8】



【図9】



THIS PAGE BLANK (USPTO)